INDIANA DATA AND COMMUNICATIONS SYSTEM

TECHNICAL AND PROCEDURAL COMMITTEE

Indiana Government Center North, 3rd Floor, 100 N. Senate Ave., Indianapolis, IN 46204-2259

IDACS TERMINAL AGENCY AGREEMENT

In accordance with 240 IAC 5-2-9, all terminal agencies and users to the IDACS system shall be required to negotiate a User Agreement with IDACS in substantially the following form:

This agreement is made and entered into the ____day of _____20___, by and between the Indiana Data and Communications System, hereinafter referred to as IDACS, and the _____, hereinafter referred to as the User Agency.

The User Agency agrees to abide by IDACS System Regulations, as well as NCIC and NLETS rules and regulations, which are hereby referenced and made a part of this agreement.

1. PURPOSE OF AGREEMENT

This agreement provides for the IDACS Committee to serve as the agency responsible for the exchange of statewide criminal offender record information and other criminal justice and law enforcement information between IDACS and the terminal agency. In addition, it provides for the Indiana State Police to serve as the state control terminal agency to facilitate the interchange of wanted file/computerized criminal history record information between NCIC and the terminal agency and message switching functions between NLETS and the terminal agency, via the IDACS network.

2. INFORMATION SERVICES

IDACS agrees to furnish the terminal agency such criminal offender record information and other criminal justice and law enforcement information as is available in the IDACS files.

IDACS further agrees to furnish such criminal history information as is available through the NCIC III (Interstate Identification Index) program to those user agencies that qualify and desire to participate in the program, and who fully meet the specific security rules pertaining to those files.

3. DEFINITION

"Access Device" and "Interface System" refer to computers, workstations, local area networks (LAN's), mobile data devices (MDD's), and other devices that are used to retrieve or enter data through the IDACS communications network.

4. MANAGEMENT CONTROL

In compliance with IDACS and NCIC policies and regulations, a criminal justice agency must have actual direct control over an interfaced system or must execute a "Management Control Agreement" if the system is to be operated by another governmental entity. A Management Control Agreement must include clear statements giving the criminal justice agency authority to set: (1) priorities, (2) standards for the selection, supervision, and termination of personnel, and (3) policies governing operations, insofar as they apply to criminal justice communications and records.

The User Agency agrees to develop, execute and maintain such "management control" over all computers, electronic equipment, software, workstations and other devices, as well as applicable personnel and organizations thereof, that provide automated access directly or indirectly to the IDACS and national systems. It is further agreed that a copy of such agreement(s) will be provided to IDACS, along with an immediate notice and copy of any future amendments thereto.

5. SECURITY

The User Agency agrees that all security requirements defined in IDACS and NCIC policies and regulations will be met. The User Agency agrees to limit access to its own employees and other governmental criminal justice officials with a specific right and need to know. Under no circumstances will non-criminal justice personnel or personnel not under the management control of the User Agency be allowed access to IDACS provided products and services. The User Agency agrees to access and use information from IDACS for official criminal justice purposes. User agency agrees to abide by the current CJIS Security Policy.

The following guidelines shall be followed to assure the security of the IDACS and national systems from unauthorized access via the Internet:

a) Access through the Internet to IDACS information is prohibited. This includes secondary dissemination of IDACS/NCIC/NLETS information through an inadequately protected communications media, such as Internet E-mail facilities and remote access file transfer.

b) Devices having access to both the Internet and the IDACS system are prohibited unless adequately protected by firewall-type devices or other superior methods. The firewall must be one certified by the International Computer Security Association (see www.icsa.net for list). In addition, the access devices with this capability must protect residual IDACS data (e.g., by removal, encryption or erasure) from subsequent Internet access.

c) Networks in which some devices have IDACS access and some devices have Internet access, such as peer-to-peer relationships and mainframes or servers that house web sites, must also be protected by firewall-type devices or other superior methods to prevent access to the IDACS system from the Internet.

6. COMMUNICATIONS LINK

User Agency will, in all cases, provide standard communication facilities as described elsewhere in this document. The communications protocol for the IDACS network is TCP/IP, and the interfaced system must appear to the IDACS system as a Datamaxx workstation. The User Agency specifically agrees to make necessary changes in its system to handle changes to the data stream, headers and/or future protocols.

7. RESPONSE TIME REQUIREMENTS

The FBI/NCIC agreement signed by IDACS defines certain processing time requirements on systems handling NCIC information. Transactions run on workstations on the interfaced system must be processed within these time limits. Accordingly, it is agreed that a workstation on an interfaced computer system must receive a response to an inquiry within 22 seconds, with 12 of the 22 seconds allocated to transmission and processing by IDACS and NCIC.

8. NOTIFICATION

In order to ensure uninterrupted service, the User Agency must provide IDACS with at least 30 days notice of changes to the User Agency's interfaced system. This includes communication lines or devices, new acquisitions, additions, deletions, as well as modifications of access devices and the selection or change of support agencies/contractors.

9. USE OF ACCESS DEVICES OR SOFTWARE NOT PROVIDED BY IDACS

For agencies converting from IDACS provided access software to software purchased or leased by the User Agency from a third party, IDACS recommends that one (1) Omnixx IDACS workstation be retained as a backup. However, this is not a requirement, except for the first two months following the implementation of a new system.

When installing new access devices, supplied by the User Agency, it is the responsibility of the User Agency, its support agency or contractor, to make any changes needed to communicate with IDACS. As the IDACS system changes, due to advancements in technology and changes in procedures, the User Agency agrees to make any needed changes to equipment and software it supplies in order to maintain communications with IDACS. IDACS will make a concerted effort to provide advanced notice to the User Agency of planned changes to the IDACS system.

In recognition of the importance of information to the criminal justice community, IDACS highly recommends that the User Agency supplied access devices be covered by twenty-four hours a day, seven days a week on-site maintenance. Acquisition of such maintenance is the responsibility of the User Agency.

The User Agency acknowledges responsibility for all hardware, operating systems, office automation, etc. supplied by the User Agency. The User Agency agrees that IDACS, or its representative support agency or contractor, can disconnect any User Agency supplied hardware or software it believes is interfering with, or prohibiting, access to the IDACS system. Whenever

possible, disconnection of hardware or software will be done after consultation with the User Agency.

The User Agency agrees to designate a technical contact person. This person will be IDACS' contact in the event of technical problems or changes. This person can be an employee of the User Agency, the support agency, or a contractor.

10. EQUIPMENT IDENTIFICATION AND LOCATION

The User Agency agrees that no access device on the interfaced system will be allowed access to IDACS unless it has been individually approved in advance by IDACS. The User Agency further agrees that no changes will be made in the locations or accessibility of any workstation without prior approval being given by IDACS. The User Agency shall maintain a site configuration diagram showing the location of all electronic devices with IDACS access. Additionally, a current system listing of all electronic devices and software with IDACS access, including the logical unit identifier must be maintained. This information shall be provided to IDACS upon request.

11. UNAPPROVED EXPANSION PROHIBITED

The User Agency agrees that no expansion allowing direct access to IDACS will be provided to any agency outside of the User Agency, unless such access is specifically approved by IDACS.

12. AUTOMATED ON-LINE TRANSACTIONS PROHIBITED

The User Agency agrees not to develop and implement batch or automated on-line transactions intended to carry out volume inquiries into the state and national systems.

13. TRAINING

The User Agency agrees to comply with all IDACS training requirements. At a minimum, the User Agency will be responsible for training their own operators on the specific and unique aspects of their own interfaced system. The agency may also assume responsibility for training related to IDACS. However, in that event the agency must: (1) develop a training program that complies with IDACS standards, (2) submit a complete description of the training and related materials to IDACS for approval, and (3) maintain records of all training provided, by individual operator, and submit proof of such training to IDACS in a form prescribed by IDACS.

14. QUALITY CONTROL, RECORD VALIDATION, AND RECORD AUDITS

The User Agency agrees to be responsible for the accuracy, completeness and timeliness of all records entered by it into the state and national files and for compliance with IDACS and NCIC record quality controls, validations and audits.

User agency further agrees to establish local procedures whereby updates to the Wanted files are reviewed for accuracy by comparing the update with supporting documentation. A person other

than the operator who accomplished the update and investigating officer who ordered it shall make this comparison.

15. PERSONNEL

Those agencies that make entries into the IDACS/NCIC Systems shall provide an operator that is certified to make entries during all normal business hours. User Agency agrees to ensure training of said personnel is in accordance with the IDACS Training and Certification Program approved by the IDACS Committee.

The User Agency agrees to require all its operators to regularly use the individual authorization procedure developed by IDACS, or by other means approved by IDACS to provide the ability to trace all transactions back to the individual that initiated the transaction.

16. 24 HOUR OPERATION AND HIT CONFIRMATION

User Agency agrees to limit the ability to enter records to only those workstations that will be manned and operational 24 hours a day, or to implement software or other procedures to handle hit confirmations 24 hours a day for any workstations not operational 24 hours a day. All unmanned devices must be logged off.

17. HELP-LINE ASSISTANCE

The Indiana State Police Data Operations Center (DOC) provides a 24-hour toll-free service number for assistance on technical and procedural problems relating to IDACS and NCIC. The User Agency is encouraged to utilize this service. However, it must be understood that IDACS personnel will not be familiar with unique or specialized features of equipment supplied by the User Agency; therefore, the assistance provided by IDACS/DOC will be very limited. In addition, if a maintenance contractor or phone company representative is dispatched to the User Agency and the problem is determined to be the fault of the User Agency supplied system, there may be a billable call that will be charged to the User Agency.

18. MOBILE DATA DEVICES (MDD)

IDACS agrees to provide, when requested, assistance on technical and operational requirements necessary to interface mobile access devices (MDD's,) to IDACS. The User Agency agrees that MDD's, installed in vehicles are subject to certain restrictions, including but not limited to:

a. All MDD's accessing IDACS will be operated only by authorized criminal justice personnel and that such mobile devices will be kept as physically secure as feasible.
b. Access by MDD's to computerized criminal history records is prohibited.
c. All MDD's accessing IDACS must provide for user authentication, data encryption, and automatic logoff functions.

19. INFORMATION SHARING

Terminal agency agrees to provide assistance as requested to those adjacent or designated law enforcement or criminal justice agencies not equipped with an IDACS terminal in accordance with IDACS Standards. This includes keeping non-terminal agency personnel informed concerning system rules, regulations, and procedures.

Such exchange of system data shall only occur when the appropriate non-terminal agency agreement has been signed.

20. DISPOSAL OF ALL MEDIA

When no longer usable, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process CJIS data shall be destroyed by shredding (which must occur before destruction), incineration, or degaussing, considering whichever method is available, appropriate, and cost effective. This list is not all-inclusive.

21. CANCELLATION

The IDACS committee may with cause, upon thirty-30 days notice in writing, cancel this agreement. The terminal agency may, upon thirty-30 days notice in writing, cancel this agreement. Upon cancellation, a terminal agency is no longer entitled to direct access to the system. Serious violations of this agreement may result in the immediate suspension of IDACS/NCIC service.

22. ACKNOWLEDGMENT

We hereby understand and acknowledge the duties; responsibilities and standards set forth in this document, as well as those documents included by reference, and will ensure that all applicable employees and support agencies and/or contractors have a full understanding of this agreement. We acknowledge that a failure to comply with the conditions of this agreement may result in administrative sanctions or penalties of law.

This agreement will become effective when executed by both parties and shall remain in force until amended or replaced.

By_____
User Agency Chief Official

Rank/Title _____

Date _____

By_____
Superintendent Indiana State Police

Date_____

By_____
Chairman, IDACS Committee

Date _____